* NOTICES *



1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

## CLAIMS

[Claim(s)]
[Claim 1]A method, wherein it is the method of providing copy protection service on a storage medium, and data on a storage medium is enciphered by a key depending on a position of data in a memory module and data is written in a position on a storage medium selected at random by each writing operation.
[Claim 2]A method according to claim 1, wherein data is arranged at a block which has a sector number and a sector number of the present or the following block is chosen from a free block list at random during each block writing.
[Claim 3]Claim 1, wherein data on a storage medium is arranged at a block and a block is enciphered by one or a key depending on a position of a block beyond it, or a method given in two.
[Claim 4]A method according to claim 3, wherein a block is enciphered by a key depending on a position of said block.
[Claim 5]A method according to claim 3, wherein a block is enciphered by a key depending on a position of a block written in before.
[Claim 6]A method according to claim 3, wherein a block is enciphered by a key depending on a position of all the blocks.
[Claim 7]A method according to claim 1, wherein a storage medium is an exchangeable solid memory module.
[Claim 8]A system arranged in order to perform a method according to claim 1 of having a control device which chooses a position at random.
[Claim 9]Playback equipment which reproduces data from a storage medium which has the data prepared in accordance with a method according to claim 1.
[Claim 10]A data accumulation medium prepared in accordance with a method according to claim 1 of having a control device which chooses a position at random.

[Translation done.]

## DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
This invention relates to a solid memory module to a data accumulation medium, especially concerning the method of providing copy protection. Probably, with the technology which progresses, next-generation portable audio reproduction and recording equipment are based on solid technology. An advantageous argument is based on consideration of weight, electric power, and a shock-proof.
[0002]
For example, a software provider like a music publisher is asking for a means for inconvenience not to completely or completely be given to an authorized user and to oppose the copy to which the information accumulated in digital one is not permitted. A method and the system must support the audition before a rental and purchase, and a business model like the controlled copy (for example, superdistribution). A specific problem is raised by the equipment according to the protection standard which can access all the information on a storage medium potentially.
[0003]
The only identification code (ID) "was engraved" in the storage medium is used for the solution of a known opposite copy. This is disadvantageous because of the consideration of privacy in a certain time. The method for which it mainly depends on such ID does not provide suitable protection against the copy machine style known as "a reproduction attack" so that it may explain below.
[0004]
So, the purpose of this invention is to provide the method and system which do not need to use comparatively inexpensive only ID which requires only moderate processing and which provide the protection especially to a reproduction attack.
[0005]
Using the key which depends for the fundamental idea of this copy protection method and a system on the position in which data is stored deterministically, data is enciphered and it combines with the method which data makes impossible [ predicting where / on a medium / it is actually accumulated ]. Therefore, a copy of data breaks change which cannot predict an accumulation position, i.i, and a relation decisive [ between the latter and a cryptographic key ] by this. So, if a code preparation method is strong enough, and a random number generator is strong enough in decryption and all the secrets are fully hidden once data is moved, it is never unrecoverable.
[0006]
Therefore, the purpose of this invention is to provide how the relation between a cryptographic key and an accumulation position is disturbed by copy operation inexpensive for storing data on a storage medium in other things.

[0007]
Especially this invention is suitable for the solid memory module which can carry out random access in every position in a memory simply based on other substance like the sector of the uniform size relevant to the access width of a bit, a byte, or the target memory.
[0008]
So, according to one feature of this invention the data on a storage medium, It is enciphered by the key K depending on the position ($L_1$, $L_2$, $L_3$) of the data on a storage medium, and data is written in the position on the storage medium selected at random by each writing operation.
[0009]
This invention relates also to the record carrier prepared by the playback equipment and the method according to claim 1 for reproducing the record prepared by the system arranged so that it may perform by the method according to claim 1, and the method according to claim 1. The further dominance feature of this invention is indicated to the independent claim.
[0010]
These and other purposes of this invention will become clear with reference to the following embodiments.
[0011]
Drawing 1 is a figure accompanied by the exchangeable module C conveyed between two the playback equipment A and B and playback equipment showing two notional playback equipment arrangement. Both playback equipment has the suitable method of inserting a module so that it may illustrate. In the following explanation, this exchangeable module presupposes that it can access by other means (for example, reading machine of a PC base). Though this does not allow the copy in which the playback equipment A and B is not accepted, it raises a risk of a copy of the data on a module not being accepted. A suitable embodiment can be used still more widely according to this invention, although it explains in relation to solid audio (solid state) playback equipment.
[0012]
It is expected that solid audio (SSA) playback equipment will be a new standard of a portable audio playback unit within several years. This is mainly because it is dominance about weight, size, used power, and shocking-proof nature to a present disk or tape. The SSA playback equipment which can be used now combines the flash memory of 32 to 64 MB and the MPEG1 layer III (MP3), or audio compression technology like AAC, in order to realize music reproduction time of CD (**) quality by 1 hour. However, the music industry requires the feature of suitable copyright protection by the ease of the copy relevant to the digital character of these pieces of equipment.
[0013]
One tool of the copy protection of digital contents is encryption. Although a code does not prevent an illegal copy in itself, since it can take out original content only by decoding using a suitable key, it cannot use such a copy and carries out it. As a result, reproduction of contents is restricted to the equipment which can access such a key. An illegal copy is prevented. it is simultaneously just, there is no inconvenience in use of the contents planned, and it is the purpose of a copy protection system to manage a key.
[0014]
The memory of most about solid multimedia accumulation application has a big flash memory and a controller on a substrate. The controller does not need to be, even if accumulated, and two or more another memories may be provided on the module. The examples of such a multimedia memory module are a memory stick (Sony), SmartMedia (SSFDC forum association), CompactFlash (registered trademark) (PCMCIA forum), and a multimediacard (MMC association). These pieces of equipment is considered as the same blocking device as a hard disk drive that memory access generates by carrying out an address

with the sector (typically 512 bytes) on a module. To be sure, the ATA interface standard of connecting a hard disk and other peripheral equipment to PC is adopted as some of above-mentioned modules. This makes it possible to use PC and to reproduce the contents of such a memory module simply (every bit). Although other modules have an interface for exclusive use and instruction set, they are based on the block. That is, the address of each sector on a module is carried out, and it may be changed.

## DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
This invention relates to a solid memory module to a data accumulation medium, especially concerning the method of providing copy protection. Probably, with the technology which progresses, next-generation portable audio reproduction and recording equipment are based on solid technology. An advantageous argument is based on consideration of weight, electric power, and a shock-proof.
[0002]
For example, a software provider like a music publisher is asking for a means for inconvenience not to completely or completely be given to an authorized user and to oppose the copy to which the information accumulated in digital one is not permitted. A method and the system must support the audition before a rental and purchase, and a business model like the controlled copy (for example, superdistribution). A specific problem is raised by the equipment according to the protection standard which can access all the information on a storage medium potentially.
[0003]
The only identification code (ID) "was engraved" in the storage medium is used for the solution of a known opposite copy. This is disadvantageous because of the consideration of privacy in a certain time. The method for which it mainly depends on such ID does not provide suitable protection against the copy machine style known as "a reproduction attack" so that it may explain below.
[0004]
So, the purpose of this invention is to provide the method and system which do not need to use comparatively inexpensive only ID which requires only moderate processing and which provide the protection especially to a reproduction attack.
[0005]
Using the key which depends for the fundamental idea of this copy protection method and a system on the position in which data is stored deterministically, data is enciphered and it combines with the method which data makes impossible [ predicting where / on a medium / it is actually accumulated ]. Therefore, a copy of data breaks change which cannot predict an accumulation position, i.i, and a relation decisive [ between the latter and a cryptographic key ] by this. So, if a code preparation method is strong enough, and a random number generator is strong enough in decryption and all the secrets are fully hidden once data is moved, it is never unrecoverable.
[0006]
Therefore, the purpose of this invention is to provide how the relation between a cryptographic key and an accumulation position is disturbed by copy operation inexpensive for storing data on a storage medium in other things.

[0007]
Especially this invention is suitable for the solid memory module which can carry out random access in every position in a memory simply based on other substance like the sector of the uniform size relevant to the access width of a bit, a byte, or the target memory.
[0008]
So, according to one feature of this invention the data on a storage medium, It is enciphered by the key K depending on the position ($L_1$, $L_2$, $L_3$) of the data on a storage medium, and data is written in the position on the storage medium selected at random by each writing operation.
[0009]
This invention relates also to the record carrier prepared by the playback equipment and the method according to claim 1 for reproducing the record prepared by the system arranged so that it may perform by the method according to claim 1, and the method according to claim 1. The further dominance feature of this invention is indicated to the independent claim.
[0010]
These and other purposes of this invention will become clear with reference to the following embodiments.
[0011]
Drawing 1 is a figure accompanied by the exchangeable module C conveyed between two the playback equipment A and B and playback equipment showing two notional playback equipment arrangement. Both playback equipment has the suitable method of inserting a module so that it may illustrate. In the following explanation, this exchangeable module presupposes that it can access by other means (for example, reading machine of a PC base). Though this does not allow the copy in which the playback equipment A and B is not accepted, it raises a risk of a copy of the data on a module not being accepted. A suitable embodiment can be used still more widely according to this invention, although it explains in relation to solid audio (solid state) playback equipment.
[0012]
It is expected that solid audio (SSA) playback equipment will be a new standard of a portable audio playback unit within several years. This is mainly because it is dominance about weight, size, used power, and shocking-proof nature to a present disk or tape. The SSA playback equipment which can be used now combines the flash memory of 32 to 64 MB and the MPEG1 layer III (MP3), or audio compression technology like AAC, in order to realize music reproduction time of CD (**) quality by 1 hour. However, the music industry requires the feature of suitable copyright protection by the ease of the copy relevant to the digital character of these pieces of equipment.
[0013]
One tool of the copy protection of digital contents is encryption. Although a code does not prevent an illegal copy in itself, since it can take out original content only by decoding using a suitable key, it cannot use such a copy and carries out it. As a result, reproduction of contents is restricted to the equipment which can access such a key. An illegal copy is prevented. it is simultaneously just, there is no inconvenience in use of the contents planned, and it is the purpose of a copy protection system to manage a key.
[0014]
The memory of most about solid multimedia accumulation application has a big flash memory and a controller on a substrate. The controller does not need to be, even if accumulated, and two or more another memories may be provided on the module. The examples of such a multimedia memory module are a memory stick (Sony), SmartMedia (SSFDC forum association), CompactFlash (registered trademark) (PCMCIA forum), and a multimediacard (MMC association). These pieces of equipment is considered as the same blocking device as a hard disk drive that memory access generates by carrying out an address

with the sector (typically 512 bytes) on a module. To be sure, the ATA interface standard of connecting a hard disk and other peripheral equipment to PC is adopted as some of above-mentioned modules. This makes it possible to use PC and to reproduce the contents of such a memory module simply (every bit). Although other modules have an interface for exclusive use and instruction set, they are based on the block. That is, the address of each sector on a module is carried out, and it may be changed.

[0015]

below a dismountable memory module is used for SSA playback equipment (refer to drawing 1) -- others (it is (for example, like the read-out machine based on PC)) -- it is accessible by a means.

[0016]

Fundamentally, two approaches exist in copy protection. The 1st is connecting an audio to specific playback equipment by supplying the only secret number used as a key for encryption of an audio to the playback equipment of each each. So, the audio accumulated on the memory with one playback equipment is reproduced only with the playback equipment. When one person has two or more SSA playback equipment, of course, it is embarrassed dramatically. To be renewable irrespective of the SSA equipment which uses the music accumulated on the memory module for downloading to the module is demanded. A user can copy audio contents to other modules, and it must be avoided that it is renewable from both.

[0017]

Although one known solution can be read from application, it is embedding the only identification code (ID) which cannot be changed at a memory module. This identification code is used for generating a cryptographic key peculiar to a module.

[0018]

Although other known solutions are inexpensive, they are using the defect in a memory module automatically generated as a result of the manufacturing process used for manufacturing the memory of high accumulation capacity. The position of these natural defects is only to each module probable.

And it works as a "fingerprint" of the equipment.

Again, the only key peculiar to a module is generated.

[0019]

These known solutions need the only identification code, and do not provide protection against a reproduction attack. 'A reproduction attack' is the form of a copy that the copy which is not observed in other systems (system 2) from one system (system 1) is made. The copy on the system (however, it is unreproducible) 2 which is not accepted may be used for recovering the refreshable copy on a system repeatedly even in even after the original copy's being invalidated.

Drawing 2 explains this in detail. To the system 1, each system has the only identification code with which it is expressed by ID1 and expressed by ID2 to the system 2, and includes the file in which contents were accumulated as a sequence of another block. In this example, the data about the right of an original copy and use is enciphered by the key obtained from ID1 and secret S. In 'a front [ purchase ] audition' or a rental business model, after the time period when access of data is still more specific, or the number of times of use is refused. The data copy (the 2nd step of drawing 2) to the system which has the only identification code ID2 does not turn into a copy which can be used. It is because an identification code is not in agreement with ID1. However, this copy is completely the same as that of an original copy (every bit). It can reverse-copy to the system 1 from the system 2 at any time, and the copy of this copy can be used. The customer with this inaccurate makes it possible to hold the copy which can be re-copied on the system 1 repeatedly, and can be used on the system 2. Therefore, after obtaining contents by "audition before purchase", an inaccurate customer

copies data to the system 2 from the system 1, and in order to maintain "an audition", he re-copies to the system 1 from the system 2 repeatedly. "An audition before purchase" turns into "an infinite audition." Similarly, this mechanism makes payment once to a rental, and may be used for copying eternally.

[0020]

In order to use a storage device effectively, it is required to use a file system. Through a file system, an user datum is systematized and is accessed. In order to treat a memory module as a blocking device, generation and management of the file system are left behind to application. In the PC environment, the operating system has already had an embedded file system support, and this is logical selection. By supporting an ATA standard, this support can be used without change to a memory module. However, in independent equipment like SSA playback equipment, when a memory module adopts the approach of a blocking device, the application needs to perform the details of a file system. So, if the controller unit on a memory module treats the details of a file system, the independent (carrying) application which needs accumulation of multimedia contents will be created still more efficiently.

[0021]

Drawing 3 shows the schematic view of Embodiment 20 of a memory module. Since it is easy, the electromechanical interface to playback equipment is not shown in a figure. The storage region 30 has the access time which became independent substantially in the physical accumulation position. The controller 22 controls access to the memory itself. The host interface 24, the memory interface 26, and various subsystems like the file system 28 are also shown. The external writing and internal selection to a memory are also shown. In application programming interface API, it should have the following functions. To the format of a memory, the arbitrary volume numbers of the random number generated whenever it is immobilization or hard wire or a command is executed by only are outputted. This number is changed only when a format instruction is executed, and thereby, all the data on equipment is lost. The copy protection itself does not need this number. In order to generate a file and to refer to the target file behind, reusable file ID is generated. When writing in a block, the sector number chosen from a free block list at random is generated. The sector number generated depending on use is a actual sector number by which the data itself was stored during writing operation, or is a sector number accumulated during the next writing operation. Among other things, since a flash memory is not barred by seek time which is common to the system based on a disk, the considerable solid audio equipment of time which is not in a loss is possible for it. Such random selection helps to equalize the consumption covering the whole element further. Application is thrown away using the sector number returned by the demanded block write instruction. When reading a block, file ID controls the output of the sector number of a block of the data itself, the present, or the next that should be read.

[0022]

Drawing 4 shows the example of the file structure distributed by the block which has the size of 512 bytes of single sector. The 1st block holds the information about a file and others have the file data itself. Above-mentioned composition blocks creation of the copy for every modular bit, unless the means of change is formed to each sector. The copy to the mid-position and the re-copy (above-mentioned "reproduction attack" is constituted) which the data on a module follows copy data to a thoroughly different position. This provides a certain protection against a copy. Copy protection is performed by enciphering a data block as a secret further by the key obtained also from the position (for example, preferably sector number) in which the data in question is stored. The information on a position is acquired from the block write-in function to return the sector number of the following file sector. Since it cannot use to the 1st block, this information may be used to data with low sensitivity. This

restriction is conquerable by making the sector number of the 1st sector in the file in which the data (for example, file information) itself is written return to a file generating function. Before reading actual data about read-out, the sector number of the present or the next can be used and application makes it possible to calculate an exactly good suitable decode key for it to solve and be alike. A cryptographic key is combined with the position of accumulation in this way, and it makes it impossible for the method of performing it to predict this position. A copy changes an accumulation position and, as a result, breaks the relation between a position and a decode key. The secret used by derivation of a key is cautious of it being shared between the secret between all the playback equipment on the whole, or a person skilled in the art occurring by other known methods.

[0023]

Drawing 5 A and 5B show the method according to this invention. It writes in the position as which the controller 22 was chosen at random in data whenever the data block was written in. In 5B, the position is indicated to be drawing 5 A by $L_1$, $L_2$, etc. Data is enciphered by the key depending on the combination of the secret S, position $L_n$, or position $L_n$ (for example, the block written in or a pre- block or written in and positions, such as a pre- block).

[0024]

It is a method which cannot reproduce the position of data and, as for creation (refer to drawing 5 B), the copy of the data of a memory module is changed. This actually occurs twice. Therefore, the re-copy of a copy has data which does not correspond to the argument which needs positions ($L_1$", $L_2$", etc.) for the suitable decipherment of data. After that, the copy of a copy is not decoded and cannot be used. "A reproduction attack" is prevented.

[0025]

Drawing 6 A and 6B show the embodiment of this invention, and are all the data (a single key ), or it consists of a block of a key -- it is enciphered by the key K, and itself is enciphered and accumulated by key K' which is an output of the hash function which has position $L_1$, $L_2$, $L_3$, etc. and the secret S as an argument. Thus, K' is dependent on the sequence of the whole by which a data block is written in the position of a data block in this case. Since position $L_1$, $L_2$, and $L_3$ are changed for every writing access by the method which cannot be predicted, thereby, key K' is changed with the result of hash function H. contents are copied, and since key K' is changed by the method which cannot be predicted when re-copied and, playback equipment goes wrong at recovery of a key (the method indicated to be drawing 5 A to 5B -- like). Therefore, any reproduction attacks go wrong. Thus, a copy is prevented by the comparatively inexpensive method which does not need to use only ID which requires only moderate processing. This invention is cautious of providing the possibility of copy protection which does not need to use only ID. The exclusion of this does not carry out use of such a code for other Reasons or the purpose of the further protection. The group of a block is able to be written [ to arrange data in the group of a block, and ] in a random position. It can be used to the group of a block instead of the same mechanism as having mentioned above being a single block. The "random position" within the concept of this invention is a large meaning, and means the position which can be beforehand predicted because of [ no ] the just purposes. "For all the just purposes", it is because a certain kind of algorithm is used and a random number or use of a position is obtained. It is preferred also about the consumption on an element to distribute equally through randomness, i.e., a memory module, truly substantially. Although it is preferred all or that a method is substantially applied to all data, this invention also includes the embodiment by which a method is applied only to some data in a memory module. This is dominance from the field of working speed, for example. The number of this inventions is one, and they are not limited to use of only one encryption method. When data is divided into a group, a different encryption method and a different method for which said encryption method depends on a

position can use it for a different group. This decreases the danger of a decipherment which is not accepted. the controller unit as which a random position is chosen although the controller is formed in the system apart from the memory module -- a memory module -- being accumulated is preferred. thereby, it becomes difficult to avoid a method or to resemble selection of the position of data and to have influence.

[0026]

It is the method of providing copy protection on a storage medium, and the position in which the data arranged at the block is stored is chosen at random by a controller (preferably inclusion), and is preferred. [ of things ] The cryptographic key for which it depends on the position of the data in a storage medium dramatically is used, and the decipherment of the copied data is made impossible in practice.

[Brief Description of the Drawings]

[Drawing 1]

It is a figure showing two notional playback equipment arrangement.

[Drawing 2]

It is a figure showing the mechanism of 'a reproduction attack' of conventional technology.

[Drawing 3]

It is a figure showing the block of the outline of the embodiment of a storage medium.

[Drawing 4]

It is a figure showing the example of a file structure.

[Drawing 5 A]

It is a figure showing how the example of the method according to this invention and this method prevent "a reproduction attack."

[Drawing 5 B]

It is a figure showing how the example of the method according to this invention and this method prevent "a reproduction attack."

[Drawing 6 A]

It is a figure showing the further example of the method according to this invention.

[Drawing 6 B]

It is a figure showing the further example of the method according to this invention.

---

[Translation done.]

* NOTICES *



1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

## DRAWINGS

[Drawing 1]

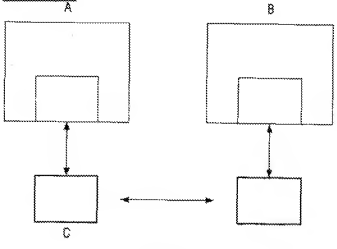
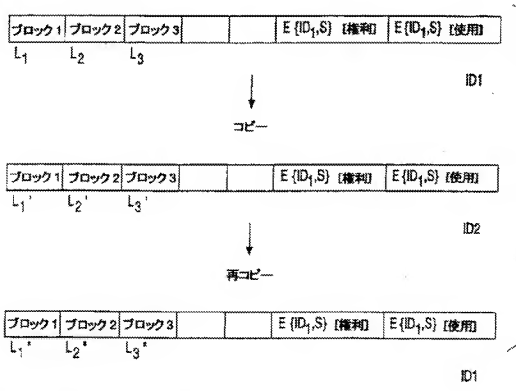
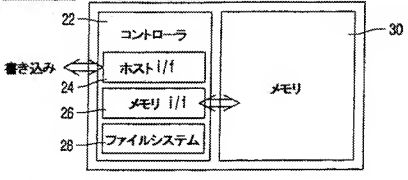



FIG. 1

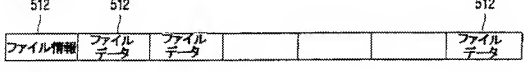
[Drawing 2]



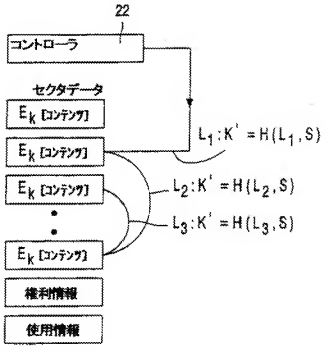

[Drawing 3]



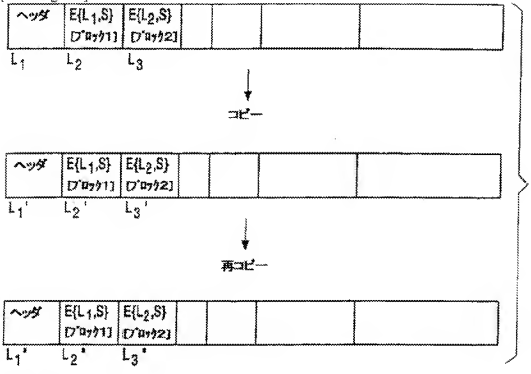

[Drawing 4]



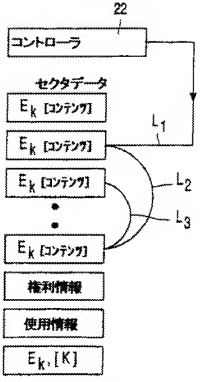

[Drawing 5 A]




[Drawing 5 B]

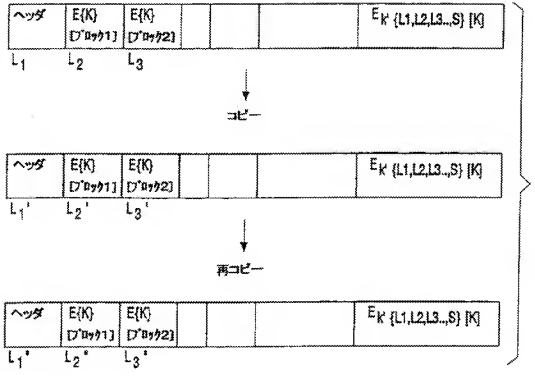



[Drawing 6 A]




$K' = H(L_1, L_2, L_3, S)$

[Drawing 6 B]



[Translation done ]

(19)日本国特許庁（ＪＰ）　(12) **公表特許公報**（Ａ）　(11)特許出願公表番号
特表2002－539557
（P2002－539557A）
(43)公表日　平成14年11月19日(2002.11.19)

| (51)Int.Cl.[7] | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｇ０６Ｆ　12/14 | ３２０ | Ｇ０６Ｆ　12/14 | ３２０Ｅ | ５Ｂ０１７ |
| | | | ３２０Ｂ | ５Ｂ０６５ |
| 3/06 | ３０４ | 3/06 | ３０４Ｍ | ５Ｄ０４４ |
| 3/08 | | 3/08 | Ｃ | |
| Ｇ１０Ｋ　15/02 | | Ｇ１０Ｋ　15/02 | | |

審査請求　未請求　予備審査請求　未請求(全 18 頁)　最終頁に続く

(21)出願番号　特願2000－605898(P2000－605898)
(86)（22)出願日　平成12年３月14日(2000.3.14)
(85)翻訳文提出日　平成12年11月14日(2000.11.14)
(86)国際出願番号　ＰＣＴ／ＥＰ００／０２２７６
(87)国際公開番号　ＷＯ００／５５７３６
(87)国際公開日　平成12年９月21日(2000.9.21)
(31)優先権主張番号　９９２００７７６．５
(32)優先日　平成11年３月15日(1999.3.15)
(33)優先権主張国　欧州特許庁（ＥＰ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＣＡ，ＪＰ，ＫＲ，ＭＸ，ＵＳ

(71)出願人　コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
Ｋｏｎｉｎｋｌｉｊｋｅ　Ｐｈｉｌｉｐｓ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｎ．Ｖ．
オランダ国　５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　１
Ｇｒｏｅｎｅｗｏｕｄｓｅｗｅｇ　１，５６２１　ＢＡ　Ｅｉｎｄｈｏｖｅｎ，Ｔｈｅ　Ｎｅｔｈｅｒｌａｎｄｓ
(72)発明者　スターリング，アントニウス　アー　エム
オランダ国，５６５６　アーアー　アインドーフェン，　プロフ・ホルストラーン　６
(74)代理人　弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】　書き込みアクセスの際に位置とキーをランダム化することによる蓄積媒体のコピー保護

(57)【要約】
蓄積媒体上にコピー保護を提供する方法であって，ブロックに配置されたデータが蓄積される位置は，（好ましくは組み込みの）コントローラによりランダムに選択されることが好ましい。蓄積媒体内のデータの位置に非常に依存している暗号化キーを使用して，コピーされたデータの解読を実際上不可能とする。

【特許請求の範囲】

【請求項１】　蓄積媒体上にコピー保護サービスを提供する方法であって、蓄積媒体上のデータは、メモリモジュール内のデータの位置に依存するキーで暗号化され、且つ、各書き込み動作で、データはランダムに選択された蓄積媒体上の位置へ書きこまれることを特徴とする方法。

【請求項２】　データはセクタ番号を有するブロックに配置され、且つ各ブロック書き込み中に、現在の又は次のブロックのセクタ番号はフリーブロックリストからランダムに選択されることを特徴とする請求項１記載の方法。

【請求項３】　蓄積媒体上のデータはブロックに配置され、且つ、ブロックは１つ又はそれ以上のブロックの位置に依存するキーで暗号化されることを特徴とする請求項１或は２記載の方法。

【請求項４】　ブロックは、前記ブロックの位置に依存するキーで暗号化されることを特徴とする請求項３記載の方法。

【請求項５】　ブロックは、前に書きこまれたブロックの位置に依存するキーで暗号化されることを特徴とする請求項３記載の方法。

【請求項６】　ブロックは、全てのブロックの位置に依存するキーで暗号化されることを特徴とする請求項３記載の方法。

【請求項７】　蓄積媒体は交換可能な固体メモリモジュールであることを特徴とする請求項１記載の方法。

【請求項８】　ランダムに位置を選択する制御装置を有する請求項１記載の方法を実行するために配置されたシステム。

【請求項９】　請求項１記載の方法に従って準備されたデータを有する蓄積媒体からデータを再生する再生装置。

【請求項１０】　ランダムに位置を選択する制御装置を有する請求項１記載の方法に従って準備されたデータ蓄積媒体。

【発明の詳細な説明】

【０００１】

本発明は、データ蓄積媒体へコピー保護を提供する方法に関し特に、固体メモリモジュールに関する。進歩する技術と共に、次世代の携帯オーディオ再生及び記録装置は、固体技術に基づくであろう。有利な議論は、重量、電力及び、耐ショックの考慮に基づく。

【０００２】

例えば、音楽出版者のようなソフトウェアプロバイダーは、許可されたユーザに少しも又は全く不便を与えない、ディジタル的に蓄積された情報の、許可されていないコピーに対抗する手段を求めている。更に、方法とシステムは、レンタル、購入前の試聴、及び、制御されたコピー（例えば、超流通）のようなビジネスモデルをサポートしなければならない。特定の問題は、蓄積媒体上の全ての情報に潜在的にアクセスできる保護規格に従っていない装置により提起される。

【０００３】

既知の対コピーの解決方法は、蓄積媒体に”刻み込まれた”唯一の識別コード（ＩＤ）を使用する。ある時点で、プライバシの考慮のために、これは不利である。さらに、以下に説明するように、そのようなＩＤに主に依存している方法は、”再生攻撃”として知られるコピー機構に対して適切な保護を提供しない。

【０００４】

それゆえ、本発明の目的は、適度な処理のみを要する比較的安価な、唯一のＩＤを使用する必要のない、特に再生攻撃に対する保護を提供する方法及びシステムを提供することである。

【０００５】

このコピー保護方法及びシステムの基本的な考えは、データが蓄積される位置に決定的に依存するキーを使用してデータは暗号化され、そして、データが媒体上のどこに実際に蓄積されるかを予測することが不可能とする方法と結合する。従って、データのコピーは蓄積位置の予測できない変更となり、これにより後者と暗号キーとの間の決定的な関係を破る。それゆえ、一度データが移動されると、暗号作成方法が十分に強く、ランダム番号発生器が暗号解読的に十分強く、そ

して、全ての秘密が十分に隠されているなら、決して回復できない。

【０００６】

従って、他のものの中で、本発明の目的は、コピー動作によって、暗号キーと蓄積位置の間の関係が乱される、蓄積媒体上にデータを蓄積するための安価な方法を提供することである。

【０００７】

本発明は、特に、ビット、バイト又は、対象のメモリのアクセス幅に関連する均一のサイズのセクタのような他の実体に基づいて、メモリ内のどの位置にも簡単にランダムアクセスできる固体メモリモジュールに好適である。

【０００８】

それゆえ、本発明の１つの特徴に従って、蓄積媒体上のデータは、蓄積媒体上のデータの位置（Ｌ１，Ｌ２，Ｌ３）に依存するキーＫで暗号化され、且つ、各書き込み動作で、データはランダムに選択された蓄積媒体上の位置へ書きこまれることを特徴とする。

【０００９】

本発明は、請求項１に記載の方法により実行されるように配置されたシステム、請求項１に記載の方法により準備された記録を再生するための再生装置及び、請求項１に記載の方法により準備される記録担体にも関連する。本発明の更なる優位な特徴は、独立請求項に記載されている。

【００１０】

本発明のこれらのそして他の目的は以下の実施例を参照して明らかとなろう。

【００１１】

図１は、２つの再生装置ＡとＢ及び、再生装置間で搬送される交換可能なモジュールＣを伴なう、概念的な２つの再生装置配置を示す図である。図示するように、両再生装置はモジュールを挿入する適切な方法を有する。以下の説明では、この交換可能なモジュールは他の手段（例えば、ＰＣベースの読み取り器）によってもアクセスできるとする。これは、再生装置ＡとＢが認められていないコピーを許さないとしても、モジュール上のデータの認められていないコピーの危険を提起する。好適な実施例は、固体オーディオ（ソリッドステート）再生装置に

関連して説明するか、本発明に従って更に広く使用し得る。

【００１２】

数年内に、固体オーディオ（ＳＳＡ）再生装置は携帯オーディオ再生装置の新たな標準となると期待されている。これは、主に、現在のディスク又は、テープに対して、重量、サイズ、使用電力及び、耐ショック性に関して優位であることによる。現在利用できるＳＳＡ再生装置は、１時間までの（近）ＣＤ品質の音楽再生時間を実現するために、３２－６４ＭＢのフラッシュメモリ及び、ＭＰＥＧ１レイヤＩＩＩ（ＭＰ３）又は、ＡＡＣのようなオーディオ圧縮技術を結合する。しかしながら、これらの装置のディジタル的性質と関連するコピーの容易さにより、音楽産業は適切な著作権保護の特徴を要求する。

【００１３】

ディジタルコンテンツのコピー保護の１つのツールは、暗号化である。暗号はそれ自身違法コピーを防止しないが、オリジナルコンテンツは適切なキーを使用して解読することによってのみ取り出せるので、そのようなコピーを使用できなくする。この結果、コンテンツの再生はそのようなキーにアクセスできる装置に制限される。違法なコピーを防止し、同時に正当なそして予定されているコンテンツの使用に不便なく、キーを管理することがコピー保護システムの目的である。

【００１４】

固体マルチメディア蓄積アプリケーションに関する大部分のメモリは、大きなフラッシュメモリと、基板上のコントローラを有する。コントローラは、集積されていてもいなくてもよく、そして、モジュール上に複数の別のメモリが設けられていても良い。そのようなマルチメディアメモリモジュールの例は、メモリスティック（ソニー）、スマートメディア（ＳＳＦＤＣフォーラムアソシエーション）、コンパクトフラッシュ（登録商標）（ＰＣＭＣＩＡフォーラム）、マルチメディアカード（ＭＭＣアソシエーション）である。さらに、これらの装置は、モジュール上のセクタ（典型的には、５１２バイト）でアドレスされることによりメモリアクセスが発生する、ハードディスクドライブと同様の、ブロック装置として考えられる。確かに、上述のモジュールの幾つかには、ハードディスク及

び、他の周辺機器をＰＣへ接続する、ＡＴＡインターフェース規格が採用されている。これは、ＰＣを使用して、そのようなメモリモジュールのコンテンツを（ビット毎に）簡単に複製することを可能とする。他のモジュールは、専用のインターフェースと命令セットを有するが、しかし、ブロックに基づいている。即ち、モジュール上の個々のセクタはアドレスされ変更され得る。

【００１５】

以下では、ＳＳＡ再生装置は、取り外し可能なメモリモジュールを採用し（図１参照）、（例えば、ＰＣに基づく読出し器のような）他の手段によりアクセス可能である。

【００１６】

基本的に、２つのアプローチがコピー保護には存在する。第１は、オーディオの暗号化のためのキーとして使用される唯一の秘密の番号を、各個々の再生装置に供給することにより特定の再生装置に、オーディオを結びつけることである。それゆえ、１つの再生装置によりメモリ上に蓄積されたオーディオは、その再生装置のみで再生される。一人が複数のＳＳＡ再生装置を有している場合には、もちろん、非常に困惑させられる。メモリモジュール上に蓄積された音楽を、そのモジュールにダウンロードするのに使用したＳＳＡ装置にかかわらず再生できることが要求される。避けられなければならないのは、ユーザがオーディオコンテンツを他のモジュールにコピーでき、そして、両方から再生できることである。

【００１７】

１つの既知の解決方法は、アプリケーションから読むことができるが、しかし、変更できない、唯一の識別コード（ＩＤ）をメモリモジュールに埋め込むことである。この識別コードは、モジュール固有の暗号化キーを発生するのに使用される。

【００１８】

他の既知の解決方法は、安価だがしかし高蓄積容量のメモリを製造するのに使用される製造プロセスの結果として自然に発生する、メモリモジュール内の欠陥を利用することである。これらの自然の欠陥の位置は、確率的に各モジュールに対して唯一であり、そして、その装置の”指紋”として働く。再び、モジュール

固有の唯一のキーが発生される。

【００１９】

これらの既知の解決方法は、唯一の識別コードを必要とし、再生攻撃に対して保護を提供しない。’再生攻撃’は、１つのシステム（システム１）から他のシステム（システム２）へ認められていないコピーがなされるコピーの形式であり、認められていない（しかし再生できない）システム２上のコピーは、元のコピーが失効後でさえも、何度も、システム上の再生可能なコピーを回復するのに使用され得る。図２は、これを詳細に説明する。各システムは、システム１に対しては、ＩＤ１により表され、システム２に対しては、ＩＤ２により表される、唯一の識別コードを有し、そして、別のブロックのシーケンスとしてコンテンツが蓄積されたファイルを含む。この例では、オリジナルコピーの権利と使用に関するデータは、ＩＤ１と秘密のＳから得られるキーで暗号化される。’購入前試聴’又は、レンタルビジネスモデルでは、さらに、データのアクセスが特定の時間期間又は使用の回数後は、拒否される。唯一の識別コードＩＤ２を有するシステムへのデータコピー（図２の第２のステップ）は、使用できるコピーとならない。識別コードがＩＤ１と一致しないからである。しかし、このコピーは、完全に（ビット毎に）オリジナルと同一である。いつでもシステム２からシステム１へ逆コピーでき、このコピーのコピーは使用できる。これは、不正な顧客は、システム１上で何度も再コピーでき且つ使用できるコピーを、システム２上で保持することを可能とする。従って、”購入前試聴”によりコンテンツを得た後に、不正の顧客はデータをシステム１からシステム２へコピーし、そして、”試聴”を維持するためにシステム２からシステム１へ何度も再コピーする。”購入前試聴”は”無限試聴”となる。同様にこの機構は、レンタルに対して１回支払いをし、そして永久にコピーするのにも使用され得る。

【００２０】

効果的に蓄積装置を使用するために、ファイルシステムを使用することが必要である。ユーザデータは、ファイルシステムを通じて組織化されかつアクセスされる。メモリモジュールをブロック装置として扱うために、ファイルシステムの生成と管理はアプリケーションに残されている。ＰＣ環境ではオペレーティング

システムは既に組み込みファイルシステムサポートを有しており、これは論理的な選択である。ＡＴＡ規格をサポートすることにより、変更無しにメモリモジュールに対してこのサポートを使用できる。しかし、ＳＳＡ再生装置のような独立の装置において、メモリモジュールがブロック装置のアプローチを採用する場合には、アプリケーションはファイルシステムの詳細を行う必要がある。それゆえ、メモリモジュール上のコントローラユニットが、ファイルシステムの詳細を扱うならば、マルチメディアコンテンツの蓄積を必要とする独立の（携帯）アプリケーションは更に効率的に作成される。

【００２１】

図３は、メモリモジュールの実施例２０の概略図を示す。簡単のために図には、再生装置への電気機械的インターフェースは示していない。蓄積領域３０は、物理的蓄積位置に実質的に独立したアクセス時間を有する。コントローラ２２は、メモリ自体へのアクセスを制御する。ホストインターフェース２４、メモリインターフェース２６及び、ファイルシステム２８のような種々のサブシステムも示されている。メモリへの、外部書き込み及び内部選択も示されている。アプリケーションプログラミングインターフェースＡＰＩ内には、以下の機能を有するべきである。メモリのフォーマットに対しては、唯一に固定の又はハードワイア又は、命令が実行されるたびに発生されるランダム番号の任意のボリューム番号が出力される。この番号は、フォーマット命令が実行されるときのみ変更され、それにより装置上の全てのデータは失われる。コピー保護自体はこの番号を必要としない。ファイルを生成するために、後に対象のファイルを参照するために、再使用可能なファイルＩＤが生成される。ブロックに書きこむときには、フリーブロックリストからランダムに選択されるセクタ番号が生成される。利用に依存して、生成されたセクタ番号は、書き込み動作中にデータ自体が蓄積された実際のセクタ番号であるか又は、次の書き込み動作中に蓄積されるセクタ番号である。他のものの間で、フラッシュメモリはディスクに基づくシステムに共通なようなシーク時間により妨げられないので、時間の相当な損失ない固体オーディオ装置が可能である。そのようなランダムの選択は、更に、全体の素子に亘る消耗を平均化することを助ける。アプリケーションは、要求されたブロック書き込み命

令により戻されたセクタ番号を使用し又は、捨てる。ブロックを読む場合に、ファイルＩＤは、データ自体と現在又は、読み出されるべき次のブロックのセクタ番号の出力を制御する。

【００２２】

図４は、５１２バイトの単一セクタのサイズを有するブロックに分散されたファイル構造の例を示す。第１のブロックは、ファイルに関する情報を保持し、他はファイルデータ自体を有する。上述の構成は、個々のセクタに対して変更の手段が設けられない限りは、モジュールのビット毎のコピーの作成をブロック化する。中間位置へのコピー及び、モジュール上のデータの続く再コピー（上述の”再生攻撃”を構成する）は、データを完全に異なる位置へコピーする。これは、コピーに対してある保護を提供する。コピー保護は、更に、秘密と、問題のデータが蓄積される位置（例えば、好ましくはセクタ番号）からも得られるキーによりデータブロックを暗号化することにより行われる。位置の情報は、次のファイルセクタのセクタ番号を戻すブロック書き込み機能から得られる。この情報は、第１ブロックに対しては利用できないので、感度の低いデータに対して使用され得る。この制限は、データ自体（例えば、ファイル情報）が書きこまれるファイル内の第１セクタのセクタ番号を、ファイル生成機能に戻させることにより克服することができる。読出しに関しては、実際のデータを読む前に、現在又は、次のセクタ番号が利用でき、アプリケーションが丁度良いときにに適切な解読キーを計算することを可能とする。暗号キーはこのように蓄積の位置と結合し、そして、それを行う方法がこの位置を予測することを不可能とする。コピーは蓄積位置を変え、そしてその結果、位置と解読キーの関係を壊す。キーの導出で使用される秘密は、全ての再生装置間の秘密で全体的に共有され、又は、当業者には既知の他の方法で発生されることに注意する。

【００２３】

図５Ａと５Ｂは、本発明に従った方法を示す。データブロックが書きこまれるたびに、コントローラ２２は、データをランダムに選択された位置へ書きこむ。図５Ａと５Ｂでは、位置は$L_1$，$L_2$等により示されている。データは秘密Ｓと位置$L_i$又は、位置$L_i$（例えば、書きこまれるブロック又は、前のブロック又

は、書きこまれ且つ前のブロック等の位置）の組合せに依存するキーで暗号化される。

【００２４】

メモリモジュールのデータのコピーを作成（図５Ｂ参照）は、データの位置を、再生できない方法で、変更する。実際これは、２回起きる。従って、コピーの再コピーは位置（Ｌ１″，Ｌ２″等）がデータの適切な解読に必要な引数に対応しないデータを有する。その後に、コピーのコピーは解読されず、使用できない。″再生攻撃″は防止される。

【００２５】

図６Ａと６Ｂは、本発明の実施例を示し、全てのデータは（単一キー又は、キーのブロックよりなる）キーＫで暗号化され、それ自身が、引数として位置Ｌ１，Ｌ２，Ｌ３等と秘密Ｓを有するハッシュ関数の出力である、キーＫ′で暗号化されて蓄積される。このように、Ｋ′は、データブロックの位置に、この場合、データブロックが書きこまれる全体のシーケンスに依存する。各書き込みアクセス毎に位置Ｌ１，Ｌ２，Ｌ３は予測できない方法で変更されるので、ハッシュ関数Ｈの結果とそれにより、キーＫ′は変更される。コンテンツがコピーされそして再コピーされる場合には、キーＫ′は予測できない方法で変更されるので、再生装置は、（図５Ａと５Ｂに示されている方法のように）キーの回復に失敗する。従って、どのような再生攻撃も失敗する。このように、コピーは、適度な処理のみを要する、唯一のＩＤを使用する必要のない、比較的安価な方法で防止される。本発明は、唯一のＩＤを使用する必要のない、コピー保護の可能性を提供することに注意する。これは、他の理由又は、更なる保護の目的でそのようなコードの使用を除外はしない。データをブロックのグループに配置すること及び、ブロックのグループがランダム位置に書き込まれることも可能である。上述したのと同じ機構が、単一ブロックの代わりに、ブロックのグループに対して使用できる。本発明の概念内の″ランダム位置″は、広い意味で、全ての正当な目的のために、予め予測できない位置を意味する。″全ての正当な目的のため″とは、ある種のアルゴリズムが使用されてランダム番号又は、位置の使用が得られることによる。実質的に真にランダム、即ち、メモリモジュールを通して実質的に等し

く分散されていることが、素子上の消耗に関しても好ましい。全ての又は実質的に全てのデータに方法が適用されることが好ましいが、本発明は、メモリモジュール内の一部のデータのみに方法が適用される実施例も包含する。これは、例えば、動作速度の面から優位である。本発明は、１つのそして１つのみの暗号化方法の使用には限定されない。データがグループに分割される場合には、異なる暗号化方法及び、前記暗号化方法が位置に依存する異なる方法が、異なるグループに使用できる。これは、認められていない解読の危険を減少する。メモリモジュールとは別にコントローラがシステム内に設けられているが、ランダム位置が選択されるコントローラユニットはメモリモジュールにと集積されているのが好ましい。これにより、方法を回避すること又は、データの位置の選択にに影響を及ぼすことが困難となる。

【００２６】

蓄積媒体上にコピー保護を提供する方法であって、ブロックに配置されたデータが蓄積される位置は、（好ましくは組み込みの）コントローラによりランダムに選択されことが好ましい。蓄積媒体内のデータの位置に非常に依存している暗号化キーを使用して、コピーされたデータの解読を実際上不可能とする。

【図面の簡単な説明】

【図１】

概念的な２つの再生装置配置を示す図である。

【図２】

従来技術の’再生攻撃’の機構を示す図である。

【図３】

蓄積媒体の実施例の概略のブロックを示す図である。

【図４】

ファイル構造の例を示す図である。

【図５Ａ】

本発明に従った方法の例とこの方法がどのように”再生攻撃”を防ぐかを示す図である。

【図５Ｂ】

本発明に従った方法の例とこの方法がどのように”再生攻撃”を防ぐかを示す図である。

【図６Ａ】

本発明に従った方法の更なる例を示す図である。

【図６Ｂ】

本発明に従った方法の更なる例を示す図である。

【図１】

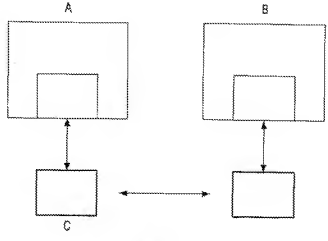
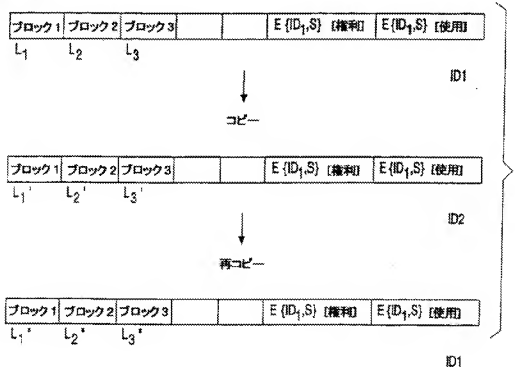
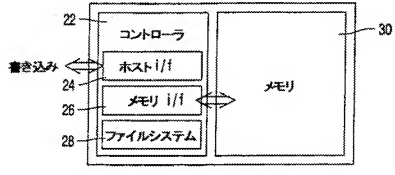



FIG. 1

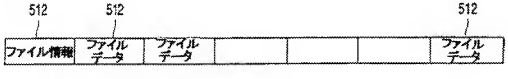
【図２】


ブロック１
ブロック２
ブロック３
E {ID1,S} [権利]
E {ID1,S} [使用]
L1
L2
L3
ID1
コピー
L1'
L2'
L3'
ID2
再コピー
L1"
L2"
L3"

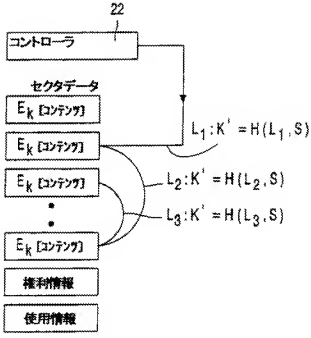
【図３】


22
コントローラ
30
書き込み
ホスト i/f
24
メモリ i/f
メモリ
26
ファイルシステム
28

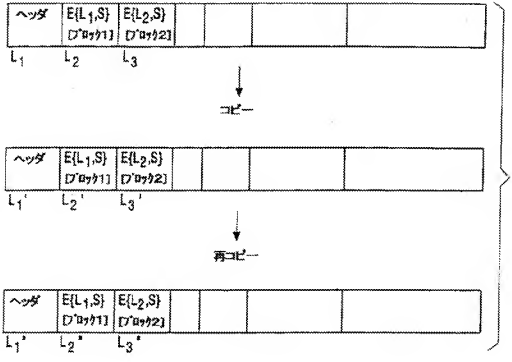
【図４】


512
512
512
ファイル情報
ファイルデータ
ファイルデータ
ファイルデータ

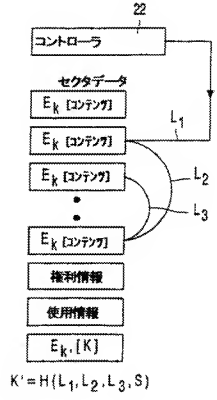
【図５Ａ】


22
コントローラ
セクタデータ
$E_k$ [コンテンツ]
$E_k$ [コンテンツ]
$E_k$ [コンテンツ]
$E_k$ [コンテンツ]
権利情報
使用情報
$L_1:K' = H(L_1, S)$
$L_2:K' = H(L_2, S)$
$L_3:K' = H(L_3, S)$

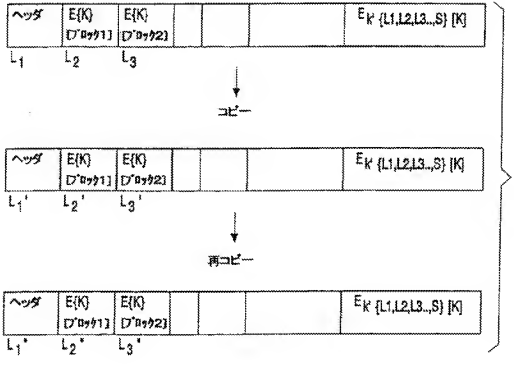
【図５Ｂ】


ヘッダ
E{L1,S} [ブロック1]
E{L2,S} [ブロック2]
L1 L2 L3
コピー
ヘッダ
E{L1,S} [ブロック1]
E{L2,S} [ブロック2]
L1' L2' L3'
再コピー
ヘッダ
E{L1,S} [ブロック1]
E{L2,S} [ブロック2]
L1'' L2'' L3''

【図６Ａ】


22
コントローラ
セクタデータ
Ek [コンテンツ]
Ek [コンテンツ]
Ek [コンテンツ]
Ek [コンテンツ]
権利情報
使用情報
Ek,[K]
L1
L2
L3
K'=H(L1,L2,L3,S)

【図６Ｂ】


ヘッダ
E{K} [ブロック1]
E{K} [ブロック2]
Ek' {L1,L2,L3..,S} [K]
L1 L2 L3
コピー
L1' L2' L3'
再コピー
L1'' L2'' L3''

【国際調査報告】

# INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/EP 00/02276

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F12/14 G11B20/00 G11B20/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G11C G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | PATENT ABSTRACTS OF JAPAN<br>vol. 013, no. 001 (P-808),<br>6 January 1989 (1989-01-06)<br>& JP 63 211045 A (TOSHIBA CORP),<br>1 September 1988 (1988-09-01)<br>abstract | 1-10 |
| A | EP 0 899 733 A (SONY DADC AUSTRIA AG)<br>3 March 1999 (1999-03-03)<br>abstract | 1-10 |
| A | PATENT ABSTRACTS OF JAPAN<br>vol. 014, no. 272 (P-1060),<br>12 June 1990 (1990-06-12)<br>& JP 02 078066 A (NEC CORP;OTHERS: 01),<br>19 March 1990 (1990-03-19)<br>abstract | 1-10 |

[ ] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 19 June 2000 | 28/06/2000 |

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer
Poth, H

Form PCT/ISA/210 (second sheet) (July 1992)

## INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/EP 00/02276

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| JP 63211045 A | 01-09-1988 | JP 2943924 B | 30-08-1999 |
| EP 0899733 A | 03-03-1999 | AU 8194998 A | 11-03-1999 |
| | | CA 2245232 A | 28-02-1999 |
| | | CN 1219728 A | 16-06-1999 |
| | | JP 11250612 A | 17-09-1999 |
| JP 02078066 A | 19-03-1990 | NONE | |

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

| (51)Int.Cl.[7] | 識別記号 | F I | | テーマコード（参考） |
|---|---|---|---|---|
| Ｇ１０Ｌ 11/00 | | Ｇ１１Ｂ 20/10 | | Ｈ |
| Ｇ１１Ｂ 20/10 | | | 20/12 | |
| 20/12 | | Ｇ１０Ｌ 9/00 | | Ｅ |
| Ｆターム（参考） | 5B017 AA03 AA06 BA07 BA09 BB00 | | | |
| | CA09 CA16 | | | |
| | 5B065 BA09 PA04 PA16 | | | |
| | 5D044 AB05 DE12 GK17 | | | |